10 MAY 1982

MEMORANDUM FOR: Industrial Security Seminar Attendees

SUBJECT: Follow-up to the Industrial Security Seminar 21-22 January 1982

1. During the Industrial Security Seminar held at Headquarters on 21 and 22 January 1982, a number of questions and comments could not be immediately answered or required further coordination. These questions and comments that required further effort have now been reviewed and in some cases action has already been taken.

2. Attached for your information is a listing of the questions raised and their current status. They are listed in the order that they were developed during the seminar and no indication of their relative importance is intended.

3. Your participation was appreciated and if questions remain or other suggestions have been developed since the seminar, please let us know.

Attachment

25X1

- There was interest in receiving security awareness material from the Agency on a continuing basis. Specifically, there is a continuing need for guest speakers, films, and briefings (slides/tapes) for security indoctrination purposes. The Agency has a very limited capability in this regard, but the Office of Security's Security Education Group (OS/SEG) will attempt to coordinate the distribution of any such material that can be identified. Specific needs should be discussed with your cognizant Industrial Security Officer for referral to SEG.

- As a result of group workshop comments regarding the audit program it was recommended that contractors be provided an audit checklist to permit them to conduct self-inspections as a security enhancement. The Industrial Security Branch (ISB) has prepared a draft checklist. The document will be complete in terms of coverage and it is being annotated to better explain the information desired. A copy will be available on request beginning 1 May 1982.

- It was also suggested that industrial security reaudits concentrate on selected areas of interest and changes since the previous audit rather than repeating the entire process. To some extent this is already done since reaudits place particular emphasis on changes that have occurred since the last audit. From a verification standpoint, however, it is necessary to include all aspects of industrial facility security during a reaudit.

- Considerable concern was expressed with regard to the experience level of Industrial Security Auditors. It was mentioned that sending new auditors to visit contractor facilities for familiarization purposes could be useful and several expressed a willingness to receive visitors for that purpose. ISB believes that this suggestion has merit and it will be considered when personnel are assigned to ISB in the future. Be assured, however, that industrial auditors receive both formal and on-the-job training prior to participating in an industrial facility audit. In addition, the junior auditor will defer to the team leader regarding any decisions affecting the contractor until his/her credentials are established.

• A number of procedural items regarding audit methodology were recommended to ISB for further consideration. Examples are: give greater emphasis to personnel security by conducting more random interviews of contractor personnel; attend actual contractor security briefings, debriefings, reindoctrinations, etc.; and concentrate on the substance of security reindoctrination programs rather than emphasis on records of attendance (paper trail). These and other related suggestions to improve the audit process are appreciated and will be incorporated into future audits wherever possible. For the record, attending briefings, etc., has been the practice and while sometimes difficult to arrange is definitely encouraged.

• During the counterintelligence presentation the limited use of the polygraph for SCI access was questioned. Specifically, it was asked why there was not a universal requirement for a polygraph test for anyone requiring SCI access. We are advised that the DCI Security Committee (SECOM) has considered this proposal but has decided against pursuing the matter further at this time. There is no question of the desirability of such a requirement and the considerations against the proposal are based on other factors, particularly resource realities.

• Also during the counterintelligence segment, participants commented that the high risk indicators (immaturity, grandiosity, psychopathy), should be questioned during background investigations and several participants requested further information on the general subject. The responsible component indicated that during the background investigation questions pertinent to immaturity, grandiosity and psychopathy are asked of the informants, not under those particular names, but in determining an individual's habits, character and reputation. Adjudication of such cases where these factors are present is often done by the Industrial Review Panel with the assistance of medical/psychiatric experts in making the security determination. The three indicators are more commonly used as descriptors in known counterintelligence cases for purposes of character assessment. Although the diagnosis of immaturity, grandiosity, and psychopathy is not a judgment that an untrained individual could make, some elements of the traits are readily apparent. The counterintelligence point to be made is that these characteristics are believed to be an indication of a high risk problem employee and Industrial Security Officers as well as supervisors and co-workers should be aware of the potential significance when these traits exist.

• Following the Information Systems Security Group's (ISSG's) computer security presentation it was suggested, and seconded by several, that ISSG establish a computer security course for industrial security managers and their associates to attend in order to keep abreast of this complex and increasingly important field. This suggestion has been acted upon and a pilot running of a 1 week course will take place in August for approximately 20 corporate security officers.

• The workshop discussions of security manuals first and foremost identified a consensus that industrial security managers should be afforded an opportunity to review and comment on proposed revisions before they are implemented. There are obvious advantages to having these views before rather than after the fact, and there is no argument in this regard. There are complex coordination problems in any effort of that type, but we will continue to support your position. The discussions of NFIB/NFIC-9.1/47 would indicate that very few implementation problems have occurred to date. Two specific questions with regard to emergency exit provisions meeting local codes, and ground level Sensitive Compartmented Information Facilities (SCIFs) having no flexibility with regard to windows, have been referred to the DCI Security Committee.

• A desire was expressed during the seminar for the publication of lists of security-approved equipment, e.g., alarm systems, telephone systems, and access control devices. The burgeoning market in these items makes it an impossible task to test and identify security-approved equipments of these types. With respect to alarm systems guidance, including specifications, has been published and disseminated in NFIB/NFIC-9.1/47. The growth in different types of telephone systems available today has been very difficult to pursue for evaluation purposes; it is realized that these new systems are very attractive and pose significant security problems. Resources are not available to test them all. Assistance is available upon request to review the security vulnerabilities of a given system. The use of access control devices is highly dependent upon the environment where they are used. First echelon guidance from the cognizant Industrial Security Officer should be able to handle questions arising as to their use. In this entire area a contractor's needs are more efficiently and effectively served through close communications with a cognizant Industrial Security Officer when purchase and installation is planned.

• Presentations on clearance, the adjudication process, and the industrial polygraph program resulted in a number of questions and comments. The first was that contractor security managers should be notified when a case is initially referred for adjudication to afford them an opportunity to withdraw the request. The answer is that due process and privacy considerations would cause a disservice to individuals if adverse information were to be passed to contractor security managers. Furthermore, in many instances such cases are resolved in the individual's favor during adjudication.

• Another questioned why polygraph results were not shared or exchanged by the two agencies participating in this program when an employee has an SCI access with one agency and is seeking another SCI access with the other agency. This is not always done because the two agencies using the polygraph use it in a different manner. One includes full lifestyle while the other limits its polygraph coverage to counterintelligence questions only, therefore, a complete exchange is not possible.

• During the seminar it was noted that DOD has initiated a practice of having background investigations conducted under contract by private firms. The question was raised whether the Agency would accept such background investigations as a basis, when necessary, to extend SCI access approvals to Agency-cognizant programs. There is no experience factor on this issue with respect to the acceptability of the product of private investigative firms. It would appear that a case-by-case approach will at least initially be needed if occasions arise involving such extensions of SCI access. The emphasis will focus on how well such investigations meet the criteria set forth in DCID No. 1/14.

• Considerable concern was expressed with regard to the requirement that contractor employees who are security disapproved and desire to appeal are told that the cognizant agency is CIA. An options paper concerning this question has been developed and is under review.

• Someone questioned why the DCI did not establish uniform standards for the conduct and adjudication of background investigations for access to SCI. The DCI established uniform standards to conduct background investigations some years ago (DCID No. 1/14). More recently the DCI Security Committee has been sponsoring Adjudicator's Seminars that have been well attended by personnel from the participating agencies that are directly involved with case adjudication. This should greatly increase the likelihood that adjudication results will be based on similar if not identical policy standards.